Doc Code: AP.PRE.REQ

PTO/SB/33 (07/05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
CH9-2000-011

I hereby certify that this corespondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR

on 5/24/2006

Signature Elaine F. Mian

Typed or printed name Elaine F. Mian

Application Number	Filed
10/058,661	1/28/2002

First Named Inventor: James F. Riordan

Art Unit	Examiner
2136	Ceervetti, David Garcia

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 43,423
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Walter J. Malinowski
Signature

Walter J. Malinowski
Typed or printed name

203-925-9400
Telephone number

May 24, 2006
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _ forms are submitted.

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:

APPLICANTS: Riordan

SERIAL NO.: 10/058,661 FILING DATE: 01/28/2002

EXAMINER: Cervetti ART UNIT: 2136

ATTORNEY'S DOCKET NO.: CH9-2000-0011US1

TITLE: EMBEDDED CRYPTOGRAPHIC SYSTEM

PRE-APPEAL BRIEF REQUEST FOR REVIEW ATTACHMENT

The following is a concise recitation of a clear error in the Examiner's rejections in this application.

ARGUMENTS

Claims 1-13 are currently pending. The Patent Office rejected claims 1, 3, 5, 7, 8, 10, 11, and 13 under 35 U.S.C. 103(a) over Kocher, U.S. Patent No. 6,327,661, in view of Tschudin, NPL Apoptosis – the Programmed Death of Distributed Services. The Patent Office rejected claims 2, 4, 6, 9, and 12 under 35 U.S.C. 103(a) over Kocher as modified by Tschudin, and further in view of Esserman.

None of the cited references - Kocher, Tschudin, or Esserman – appear to disclose or fairly suggest the claimed subject matter of **"switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6)"** in conjunction with either the claimed subject matter of **"checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i"** or **"stop said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i."**

Applicant's invention concerns plaintext, ciphertext test pairs and is directed to a method

for detecting compromise of cryptographic operations because the ciphertext generated by a first cryptographic algorithm from a test plaintext indicates that an apoptosis key has been used (page 4, lines 3-5 and 24-27). Upon detection of an apoptosis key by the generation of ciphertext corresponding to that apoptosis key encrypting the designated plaintext, cryptographic algorithms should be switched and a more conservative algorithm should be used (page 4, lines 27-35, of Applicant's specification). An advantage of the solution of the present invention is "that there is no need for controlling respectively trusting the manufacturer or a security service" (page 5, lines 11-12, of Applicant's specification).

The Patent Office asserted (page 4-5 of the Final Office Action mailed January 24, 2006) asserted that the following passages of Kocher disclose the claimed invention, at least regarding claim 1: column 2, lines 60-67; column 13, lines 20-67; column 14, lines 1-67. In none of these passages does there appear to be a disclosure of stopping a first cryptographic algorithm, performing any activity with respect to a first cryptographic algorithm, or switching to a second cryptographic algorithm.

Kocher (column 13, lines 20-67) discloses "Cryptographic operations should normally be checked to ensure that incorrect computations do not compromise keys or enable other attacks. Cryptographic implementations of the present invention can be, and in a preferred embodiment are, combined with error-detection and/or error-correction logic to ensure that cryptographic operations are performed correctly. For example, a simple and effective technique is to perform cryptographic operations twice, ideally using two independent hardware processors and/or software implementations, with a comparison operation performed at the end to verify that both produce identical results. **If the results produced by the two units do not match, the failed comparison will prevent the defective processing result from being used.** In situations where security is more important than reliability, **if the compare operation ever fails (or fails too many times) the device may self-destruct (such as by deleting internal keys) or disable itself.** For example, a device might erase its key storage memory if either two defective DES operations occur sequentially or five defective DES results occur during the lifetime of the device. In some cryptosystems, full redundancy is not necessary. For example, with RSA, methods are known in the background art for self-checking functions that can be incorporated into the cryptosystem

implementation (e.g., RSA signatures can be verified after digital signing operations). Detection of conditions likely to cause incorrect results may also be used. In particular, active or passive sensors to detect unusually high or low voltages, high-frequency noise on voltage or signal inputs, exposure to electromagnetic fields and radiation, and physical tampering may be employed. **Inappropriate operating conditions can (for example) trigger the device to reset, delete secrets, or self-destruct.** Self-diagnostic functions such as a POST (power-on-self-test) should also be incorporated to verify that cryptographic functions have not been damaged. In cases where an ATR (answer-to-reset) must be provided before a comprehensive self-test can be completed, the self-test can be deferred until after completion of the first transaction or until a sufficient idle period is encountered. For example, a flag indicating successful POST completion can be cleared upon initialization. While the card is waiting for a command from the host system, it can attempt the POST. Any I/O received during the POST will cause an interrupt, which will cancel the POST (leaving the POST-completed flag at zero). If any cryptographic function is called, the device will check the POST flag and (if it is not set) perform the POST before doing any cryptographic operations."

Kocher discloses a defective processing result may be prevented from being used, resetting the device, deleting secrets by the device, or the device self-destructing. All claims recite that the first cryptographic algorithm is stopped if the test ciphertext is enciphered from the test plaintext when using the apoptosis key. As the base reference, Kocher does not seem amenable to having multiple cryptographic algorithms in a single embodiment or stopping a cryptographic algorithm where the test ciphertext has been enciphered from the test plaintext when using the apoptosis key.

Tschudin does disclose apoptosis of distributed services, but seems not to disclose or fairly suggest that the apoptosis of distributed services may entail the stopping of a cryptographic algorithm if the test ciphertext is the enciphered image of a test plaintext when using the apoptosis key.

Esserman does disclose selectively terminating the transmission of signals under a particular algorithm in a subscription television system and providing a replacement algorithm (col. 6, lines 54-58), but seems not to disclose or fairly suggest that the apoptosis of distributed

services may entail the stopping of a cryptographic algorithm if the test ciphertext is the enciphered image of a test plaintext when using the apoptosis key.

In summary, **none of the references Kocher, Tschudin, or Esserman disclose or suggest the claimed technique where a first cryptographic algorithm is stopped when a test plaintext generates a corresponding test ciphertext under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i.**

Also, claims 2, 4, 6, 7, 9, and 12 present subject matter not made obvious by the prior art of record. The subject matter of these claims recites a second cryptographic algorithm that is switched to from the first cryptographic algorithm, a cascaded list of different algorithms, or publishing at least one test plaintext and for each test plaintext publishing the corresponding test ciphertext. **Would one of ordinary skill in the art seek to modify the smart card system of Kocher to use a second or different cryptographic algorithm or to publish a test ciphertext and corresponding test ciphertext?**

Thus, claims 1, 3, 5, 7, 8, 10, 11, and 13 are not made obvious by Kocher in view of Tschudin and claims 2, 4, 6, 9, and 12 are not made obvious by Kocher, Tschudin, or Esserman, alone or in combination.

Respectfully submitted:

Walter J. Malinowski May 24, 2006

Walter J. Malinowski Date
Reg. No.: 43,423

Customer No.: 29683

HARRINGTON & SMITH, LLP
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203)925-9400, extension 19
Facsimile: (203)944-0245
email: wmalinowski@hspatent.com